Advisory
Title: W32/Mimail Virus
Date August 2, 2003

SYSTEMS AFFECTED: Computers using the following operating systems:

* Microsoft Outlook Express 6.0 SP1, when used with:
  - the operating system: Microsoft Windows XP SP1
  - the operating system: Microsoft Windows Millennium Edition
  - the operating system: Microsoft Windows 2000 SP2
  - the operating system: Microsoft Windows 98 Second Edition
  - the operating system: Microsoft Windows NT 4.0 SP6a
* Microsoft Outlook Express 6.0, when used with:
  - the operating system: Microsoft Windows XP
* Microsoft Outlook Express 5.5 for Windows 98 Second Edition
* Microsoft Outlook Express 5.5 for Windows Millennium Edition
* Microsoft Outlook Express 5.5 for Windows 2000
* Microsoft Outlook Express 5.5 for Windows NT 4.0

OVERVIEW

On Friday, August 1st 2003 The Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSD) began to receive reports of a new mass mailing virus, now referred to as W32/Mimail, spreading on the Internet.

DESCRIPTION

The W32/Mimail virus is a malicious file attachment containing a specially crafted MHTML file named 'message.html'. This file is delivered inside of a .ZIP archive file named 'message.zip'. Viewing the 'message.html' file on a vulnerable system will cause the malicious code to be installed and executed. The malicious code is a mass-mailer.

The malicious code is installed and runs as %windowsroot%\videodrv.exe. The recipients are determined by scanning files in C:\Documents and Settings\{current_user}\ , C:\Program Files\ and C:\%windowsroot%\Fonts\ for the pattern %s@%s and stores this information in %windowsroot%\eml.tmp.

Anti-virus vendors have developed signatures for W32/Mimail which can be found at:
http://www.sarc.com/avcenter/venc/data/w32.mimail.a@mm.html
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MIMAIL.A
http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100523

The vulnerability which was identified in April 2003, makes it possible for W32/Mimail to execute automatically once the .ZIP archive is opened is described in Vulnerability Note VU#208052 and Microsoft Security Bulletin MS03-014.

RECOMMENDATION
DHS/IAIP encourages sites to review Microsoft Security Bulletin MS03-014 and apply the Cumulative Patch for Outlook Express (220994).

Run and maintain an anti-virus product

While an up-to-date antivirus software package cannot protect against all malicious code, for most users it remains the best first-line of defense against malicious code attacks.

Most antivirus software vendors release frequently updated information, tools, or virus databases to help detect and recover from malicious code, including W32/Mimail. Therefore, it is important that users keep their antivirus software up to date.

Many antivirus packages support automatic updates of virus definitions. DHS/IAIP recommends using these automatic updates when available.

Do not run programs or open files of unknown origin. Email users should be wary of unexpected attachments or unusual links contained in email. Never download, install, run or open a program or file unless you know it to be authored by a person or company that you trust.

Filter the email, sites can use email filtering techniques to delete messages known to contain this malicious code, or they can filter all attachments.

Advisories recommend the immediate implementation of protective actions, including best practices when available. DHS encourages recipients of this advisory to report information concerning suspicious or criminal activity to law enforcement or a DHS watch office. The DHS Information Analysis and Infrastructure Protection watch offices may be contacted at:

For private citizens and companies –	Phone: (202) 323-3205, 1-888-585-9078,
	Email: nipc.watch@fbi.gov;
	Online: http://www.nipc.gov/incident/cirr.htm
For telecommunications industry -	Phone: (703) 607-4950
	Email: ncs@dhs.gov
For Federal agencies/departments -	Phone: (888) 282-0870
	Email: fedcirc@fedcirc.gov
	Online: https://incidentreport.fedcirc.gov

DHS intends to update this alert should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) is anticipated; the current HSAS level is YELLOW.